

On the 2-part of the Birch-Swinnerton-Dyer conjecture for elliptic curves with complex multiplication

John Coates, Minhyong Kim ^{*}, Zhibin Liang [†], Chunlai Zhao [‡]

April 9, 2013

To Peter Schneider for his 60th birthday

1 Introduction

Let E be an elliptic curve defined over \mathbb{Q} , with complex multiplication by the ring of integers of an imaginary quadratic field K . Thus, by the theory of complex multiplication, K must be either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, or one of the fields

$$(1) \quad \mathbb{Q}(\sqrt{-q}) \quad (q = 7, 11, 19, 43, 67, 163).$$

Recently, Y. Tian [6], [7] made the remarkable discovery that one could prove deep results about the arithmetic of certain quadratic twists of E with root number -1 , by combining formulae of Gross-Zagier type for these twists, with a weak form of the 2-part of the conjecture of Birch and Swinnerton-Dyer for certain other quadratic twists of E , where the root number is $+1$. We recall that, when the complex L -series of an elliptic curve with complex multiplication does not vanish at $s = 1$, the p -part of the conjecture of Birch and Swinnerton-Dyer has been established, by the methods of Iwasawa theory, for all primes p which do not divide the order of the group of roots of unity of K (see [5]). However, at present we do not know how to extend such methods to cover the case of the prime $p = 2$. Nevertheless, when $K = \mathbb{Q}(\sqrt{-1})$, one of us [9], [10], [11], [12] did establish a weaker result in this direction for the prime $p = 2$, by combining the classical expression for the value of the complex L -series as a sum of Eisenstein series (see Corollary 2.2), with an averaging argument over quadratic twists, and happily this weaker result has sufficed for Tian's work in [6], [7]. The aim of the present note is to show that the rather elementary method developed in the papers [9], [10], [11], [12] works even more simply for quadratic twists of those elliptic curves E having good reduction at the prime 2, and with complex multiplication by the ring of integers of the fields K given by (1).

^{*}Supported by EPSRC grant EP/G024979/2

[†]Supported by NSFC11001183 and NSFC11171231.

[‡]Supported by NSFC01272499.

We hope that one can use some of the weak forms of the 2-part of the conjecture of Birch and Swinnerton-Dyer established here (see, in particular, our Corollary 4.6) to extend the deep results of [6], [7], [8], to certain infinite families of quadratic twists of our curves E , having root number equal to -1 . It is also interesting to note that, in [8], Tian and his collaborators introduce a new and completely different method for establishing weak forms of the 2-part part of the conjecture of Birch and Swinnerton-Dyer for curves with $K = \mathbb{Q}(\sqrt{-1})$, by using a celebrated formula of Waldspurger, and they believe that this new method can eventually be applied to a much wider class of elliptic curves, including those without complex multiplication. Needless to say, the rather elementary methods used here seem to be special to elliptic curves with complex multiplication. Finally, we wish to thank Y. Tian for his ever helpful comments on our work.

2 The averaging argument

Let K be an imaginary quadratic field of class number 1, which we assume is embedded in \mathbb{C} , and let \mathcal{O}_K its ring of integers. Let E be any elliptic curve defined over K , whose endomorphism ring is isomorphic to \mathcal{O}_K . Fix once and for all a global minimal generalized Weierstrass equation for E over \mathcal{O}_K

$$(2) \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in \mathcal{O}_K).$$

Let \mathfrak{L} be the period lattice of the Neron differential $dx/(2y + a_1x + a_3)$. Then \mathfrak{L} is a free \mathcal{O}_K -module of rank 1, and we fix $\Omega_\infty \in \mathbb{C}^\times$ such that $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$. Denote by ψ_E the Grossencharacter of E/K in the sense of Deuring-Weil, and write \mathfrak{f} for the conductor of ψ_E (thus the prime divisors of \mathfrak{f} are precisely the primes of K where E has bad reduction). Now let \mathfrak{g} be any integral multiple of \mathfrak{f} , and fix $g \in \mathcal{O}_K$ such that $\mathfrak{g} = g\mathcal{O}_K$. Let S be the set of primes ideals of K dividing \mathfrak{g} , and denote by

$$L_S(\bar{\psi}_E, s) = \sum_{(\mathfrak{a}, \mathfrak{g})=1} \frac{\bar{\psi}_E(\mathfrak{a})}{(N\mathfrak{a})^s}$$

the imprimitive Hecke L -function of the complex conjugate Grossencharacter of ψ_E . Our subsequent induction argument is based on the following expression for $L_S(\bar{\psi}_E, s)$, which goes back to the 19th century. Let z and s be complex variables. For any lattice L in the complex plane \mathbb{C} , define the Kronecker-Eisenstein series by

$$H_1(z, s, L) := \sum_{w \in L} \frac{\bar{z} + \bar{w}}{|z + w|^{2s}},$$

where the sum is taken over all $w \in L$, except $-z$ if $z \in L$. This series converges to define a holomorphic function of s in the half plane $\operatorname{Re}(s) > 3/2$, and it has an analytic continuation to the whole s -plane. Let \mathfrak{R} denote the ray class field of K modulo \mathfrak{g} , and let \mathcal{B} be any set of integral ideals of K , prime to \mathfrak{g} , whose Artin symbols give precisely the Galois group of \mathfrak{R} over K (in other words, \mathcal{B} is a set of integral ideals of K representing

the ray class group of K modulo \mathfrak{g}). Since the conductor of ψ_E divides \mathfrak{g} , it is well known that \mathfrak{R} is equal to the field $K(E_g)$, which is obtained by adjoining to K the coordinates of the g -division points on E .

Proposition 2.1. *We have*

$$L_S(\bar{\psi}_E, s) = \frac{|\Omega_\infty/g|^{2s}}{(\Omega_\infty/g)} \sum_{\mathfrak{b} \in \mathcal{B}} H_1(\psi_E(\mathfrak{b})\Omega_\infty/g, s, \mathfrak{L}).$$

Proof. As mentioned above \mathcal{B} is a set of integral representatives of the ray class group of K modulo \mathfrak{g} , and so it follows that, fixing any generator of each \mathfrak{b} in \mathcal{B} , we obtain a set of representatives of $(\mathcal{O}/\mathfrak{g})^*/\tilde{\mu}_K$, where $\tilde{\mu}_K$ denotes the image under reduction modulo \mathfrak{g} of the group μ_K of roots of unity of K . Moreover, the very existence of ψ_E shows that the reduction map from μ_K to $\tilde{\mu}_K$ must be an isomorphism of groups. For each \mathfrak{b} in \mathcal{B} , we choose the generator of \mathfrak{b} given by $\psi_E(\mathfrak{b})$. It follows that, as \mathfrak{b} runs over \mathcal{B} and c runs over \mathfrak{g} , the principal ideals $(\psi_E(\mathfrak{b}) + c)$ run over all integral ideals of K , prime to \mathfrak{g} , precisely once. Thus

$$L_S(\bar{\psi}_E, s) = \sum_{\mathfrak{b} \in \mathcal{B}} \sum_{c \in \mathfrak{g}} \frac{\bar{\psi}_E((\psi_E(\mathfrak{b}) + c))}{|\psi_E(\mathfrak{b}) + c|^{2s}}.$$

Note that, since $c \in \mathfrak{g}$, we have

$$(\psi_E(\mathfrak{b}) + c) = (\psi_E(\mathfrak{b}))(1 + c/\psi_E(\mathfrak{b})) = \mathfrak{b}(1 + c/\psi_E(\mathfrak{b})),$$

so that

$$\bar{\psi}_E((\psi_E(\mathfrak{b}) + c)) = \bar{\psi}_E(\mathfrak{b})(1 + c/\psi_E(\mathfrak{b})) = \bar{\psi}_E(\mathfrak{b}) + c.$$

Hence

$$L_S(\bar{\psi}_E, s) = \sum_{\mathfrak{b} \in \mathcal{B}} \sum_{c \in \mathfrak{g}} \frac{\overline{\psi_E(\mathfrak{b}) + c}}{|\psi_E(\mathfrak{b}) + c|^{2s}},$$

which can easily be rewritten as

$$\frac{|\Omega_\infty/g|^{2s}}{(\Omega_\infty/g)} \sum_{\mathfrak{b} \in \mathcal{B}} \sum_{w \in \mathfrak{L}} \frac{\overline{\psi_E(\mathfrak{b})\Omega_\infty/g + w}}{|\psi_E(\mathfrak{b})\Omega_\infty/g + w|^{2s}},$$

completing the proof of the theorem. \square

We recall that, for any lattice L , the non-holomorphic Eisenstein series $\mathcal{E}_1^*(z, L)$ is defined by

$$\mathcal{E}_1^*(z, L) = H_1(z, 1, L).$$

Then the above proposition immediately implies that

$$L_S(\bar{\psi}_E, 1)/\Omega_\infty = g^{-1} \sum_{\mathfrak{b} \in \mathcal{B}} \mathcal{E}_1^*(\psi_E(\mathfrak{b})\Omega_\infty/g, \mathfrak{L}).$$

Also, it is well known (see, for example, [2]) that $\mathcal{E}_1^*(\psi_E(\mathfrak{b})\Omega_\infty/g, \mathfrak{L})$ belongs to the field \mathfrak{K} , and satisfies

$$\mathcal{E}_1^*(\psi_E(\mathfrak{b})\Omega_\infty/g, \mathfrak{L}) = \mathcal{E}_1^*(\Omega_\infty/g, \mathfrak{L})^{\sigma_{\mathfrak{b}}},$$

where $\sigma_{\mathfrak{b}}$ denotes the Artin symbol of \mathfrak{b} in the Galois group of \mathfrak{K} over K . Thus the above proposition has the following immediate corollary, where $Tr_{\mathfrak{K}/K}$ denotes the trace map from \mathfrak{K} to K .

Corollary 2.2. *We have*

$$L_S(\bar{\psi}_E, 1)/\Omega_\infty = Tr_{\mathfrak{K}/K}(g^{-1}\mathcal{E}_1^*(\Omega_\infty/g, \mathfrak{L})).$$

We next consider the twisting of E by certain quadratic extensions of K . A non-zero element M of \mathcal{O}_K is said to be square free if it is not divisible by the square of any non-unit element of this ring.

Lemma 2.3. *Let M be any non-zero and non-unit element of \mathcal{O}_K , which satisfies (i) M is square free, (ii) M is prime to the discriminant of K , and (iii) $M \equiv 1 \pmod{4}$. Then the extension $K(\sqrt{M})/K$ has conductor equal to $M\mathcal{O}_K$.*

Proof. Since M is square free and $M \equiv 1 \pmod{4}$, the extension $K(\sqrt{M})/K$ is totally and tamely ramified at all primes dividing M . Thus the assertion of the lemma will follow once we have shown that the primes of K above 2 are not ramified in this extension. Let v be any place of K above 2. Let w be such that $w^2 = M$, and put $z = (w-1)/2$. Then z is a root of the polynomial $f(X) = X^2 - X - (M-1)/4$, so that z is an algebraic integer. But $f'(z) = 2z - 1$ is then clearly a unit at v , and so v is unramified in our extension $K(\sqrt{M})/K$, completing the proof. \square

Let M be as in the above lemma, and assume in addition that $(M, \mathfrak{f}) = 1$. We write χ_M for the abelian character of K defining the quadratic extension $K(\sqrt{M})/K$, and let $E^{(M)}$ denote the twist of E by χ_M . Thus $E^{(M)}$ is the unique elliptic curve defined over K , which is isomorphic to E over $K(\sqrt{M})$, and which is such that

$$E^{(M)}(K) = \{P \in E(K(\sqrt{M})) : \sigma(P) = \chi_M(\sigma)(P), \sigma \in Gal(K(\sqrt{M})/K)\}.$$

The curve $E^{(M)}$ also has endomorphism ring isomorphic to \mathcal{O}_K , and its Grossencharacter, which we denote by $\psi_{E^{(M)}}$, is equal to the product $\psi_E \chi_M$. We write \mathfrak{f}_M for the conductor of $\psi_{E^{(M)}}$. In view of the above lemma, we have $\mathfrak{f}_M = M\mathfrak{f}$, because $(\mathfrak{f}, M) = 1$ and χ_M has conductor $M\mathcal{O}_K$. Finally, putting

$$\mathfrak{p}(z, \mathfrak{L}) = x + (a_1^2 + 4a_2)/12, \mathfrak{p}'(z, \mathfrak{L}) = 2y + a_1x + a_3,$$

we obtain a classical Weierstrass equation for E over \mathbb{C} of the form

$$Y^2 = 4X^3 - g_2(\mathfrak{L})X - g_3(\mathfrak{L}),$$

with $X = \mathbf{p}(z, \mathfrak{L})$, $Y = \mathbf{p}'(z, \mathfrak{L})$. The corresponding classical Weierstrass equation for $E^{(M)}$ over \mathbb{C} is then given by

$$Y^2 = 4X^3 - M^2 g_2(\mathfrak{L})X - M^3 g_3(\mathfrak{L}).$$

Hence the period lattice for the curve $E^{(M)}$ over \mathbb{C} is given by

$$(3) \quad \mathfrak{L}_M = \frac{\Omega_\infty}{\sqrt{M}} \mathcal{O}_K.$$

We now suppose that we are given an infinite sequence

$$\pi_1, \pi_2, \dots, \pi_n, \dots$$

of distinct prime elements of \mathcal{O}_K . We shall say that this sequence is *admissible* for E/K if, for all $n \geq 1$, we have that π_n is prime to the discriminant of K , and

$$(4) \quad \pi_n \equiv 1 \pmod{4}, \quad (\pi_n, \mathfrak{f}) = 1.$$

For each integer $n \geq 0$, define

$$(5) \quad \mathcal{M}_n = \pi_1 \cdots \pi_n, \quad \mathfrak{g}_n = \mathcal{M}_n \mathfrak{f}.$$

We now take \mathfrak{R}_n to be the ray class field of K modulo \mathfrak{g}_n . Since $\pi_j \equiv 1 \pmod{4}$, the above lemma shows that the extension $K(\sqrt{\pi_j})/K$ has conductor $\pi_j \mathcal{O}_K$, and so is contained in \mathfrak{R}_n , for all j with $1 \leq j \leq n$. Hence the field \mathfrak{J}_n defined by

$$(6) \quad \mathfrak{J}_n = K(\sqrt{\pi_1}, \dots, \sqrt{\pi_n})$$

is always a subfield of \mathfrak{R}_n . Let S_n be the set of prime ideals of K dividing \mathfrak{g}_n . Also, writing f for any \mathcal{O}_K generator of the ideal \mathfrak{f} , we put $g_n = f \mathcal{M}_n$, so that $\mathfrak{g}_n = g_n \mathcal{O}_K$. Finally, we define \mathcal{D}_n to be the set of all divisors of \mathcal{M}_n which are given by the product of any subset of $\{\pi_1, \dots, \pi_n\}$. The averaging theorem which follows is essentially contained in the earlier paper of one of us [9], and is the basis of all of our subsequent arguments. For simplicity, we write just ψ_M for the Grossencharacter of the curve $E^{(M)}$ for any $M \in \mathcal{D}_n$.

Theorem 2.4. *Let $\{\pi_1, \dots, \pi_n, \dots\}$ be any admissible sequence for E/K . Then, for all integers $n \geq 1$, we have*

$$(7) \quad \sum_{M \in \mathcal{D}_n} L_{S_n}(\bar{\psi}_M, 1) / \Omega_\infty = 2^n \text{Tr}_{\mathfrak{R}_n / \mathfrak{J}_n} (g_n^{-1} \mathcal{E}_1^*(\Omega_\infty / g_n, \mathfrak{L})),$$

where $\text{Tr}_{\mathfrak{R}_n / \mathfrak{J}_n}$ denotes the trace map from \mathfrak{R}_n to \mathfrak{J}_n .

Proof. Let M be any element of \mathcal{D}_n . Applying Corollary 2.2 to the curve $E^{(M)}$ with $\mathfrak{g} = \mathfrak{g}_n$, and using (3), we conclude that

$$L_{S_n}(\bar{\psi}_M, 1)\sqrt{M}/\Omega_\infty = \text{Tr}_{\mathfrak{R}_n/K}(g_n^{-1}\mathcal{E}_1^*(\frac{\Omega_\infty}{\sqrt{M}g_n}, \mathfrak{L}_M)).$$

Now, for any non-zero complex number λ , we have

$$\mathcal{E}_1^*(z, \mathfrak{L}_M) = \lambda \mathcal{E}_1^*(\lambda z, \lambda \mathfrak{L}_M).$$

Hence, taking $\lambda = \sqrt{M}$, and writing G_n for the Galois group of \mathfrak{R}_n/K , we conclude that

$$(8) \quad L_{S_n}(\bar{\psi}_M, 1)/\Omega_\infty = \sum_{\sigma \in G_n} (\sqrt{M})^{\sigma-1} g_n^{-1} (\mathcal{E}_1^*(\Omega_\infty/g_n, \mathfrak{L}))^\sigma.$$

It is now clear that the assertion of the theorem is an immediate consequence of the following lemma. \square

Lemma 2.5. *Let $H_n = \text{Gal}(\mathfrak{R}_n/\mathfrak{J}_n)$. If σ is any element of G_n , then $\sum_{M \in \mathcal{D}_n} (\sqrt{M})^{\sigma-1}$ is equal to 2^n if σ belongs to H_n , and is equal to 0 otherwise.*

Proof. The first assertion of the lemma is clear. To prove the second assertion, suppose that σ maps $k \geq 1$ elements of the set $\{\sqrt{\pi_1}, \dots, \sqrt{\pi_n}\}$ to minus themselves, and write $V(\sigma)$ for the subset consisting of all such elements. If M be any element of \mathcal{D}_n , it is clear that σ will fix \sqrt{M} if and only if M is a product of an even number of elements of $V(\sigma)$, with an arbitrary number of elements of the complement of $V(\sigma)$ in $\{\sqrt{\pi_1}, \dots, \sqrt{\pi_n}\}$. Hence the total number of M in \mathcal{D}_n such that σ fixes \sqrt{M} is equal to

$$2^{n-k}((k, 0) + (k, 2) + (k, 4) + \dots) = 2^{n-1},$$

where (n, r) denotes the number of ways of choosing r objects from a set of n objects. Similarly, the total number of M in \mathcal{D}_n such that σ maps \sqrt{M} to $-\sqrt{M}$ is equal to

$$2^{n-k}((k, 1) + (k, 3) + (k, 5) + \dots) = 2^{n-1}.$$

Since these last two expressions are equal, the second assertion of the lemma is now clear. \square

3 Integrality at 2

We use the notation and hypotheses introduced in the last section. Our aim in this section is to prove the following result.

Theorem 3.1. *Assume that E has good reduction at the primes of K above 2, and that $\{\pi_1, \dots, \pi_n, \dots\}$ is any admissible sequence for E/K . For all $n \geq 1$, define*

$$\Psi_n = \text{Tr}_{\mathfrak{R}_n/\mathfrak{J}_n}(g_n^{-1}\mathcal{E}_1^*(\frac{\Omega_\infty}{g_n}, \mathfrak{L})).$$

Then $2\Psi_n$ is always integral at all places of \mathfrak{J}_n above 2. Moreover, if the coefficient a_1 in (2) is divisible by 2 in \mathcal{O}_K , then Ψ_n is integral at all places of \mathfrak{J}_n above 2.

Before giving the proof of the theorem, we recall some classical identities involving elliptic functions (see. for example, [1]). Let L be any lattice in the complex plane, and write $\mathfrak{p}(z, L)$ for the Weierstrass \mathfrak{p} -function attached to L . For each integer $m \geq 2$, we define the elliptic function $B_m(z, L)$ by

$$2B_m(z, L) = \frac{\mathfrak{p}''(z, L)}{\mathfrak{p}'(z, L)} + \sum_{k=2}^{k=m-1} \frac{\mathfrak{p}'(kz, L) - \mathfrak{p}'(z, L)}{\mathfrak{p}(kz, L) - \mathfrak{p}(z, L)}.$$

Lemma 3.2. *For all integers $m \geq 2$, we have*

$$B_m(z, L) = \mathcal{E}_1^*(mz, L) - m\mathcal{E}_1^*(z, L).$$

Proof. Let $\zeta(z, L)$ denote the Weierstrass zeta function of L . The following identity is classical

$$\mathcal{E}_1^*(z, L) = \zeta(z, L) - zs_2(L) - \bar{z}A(L)^{-1},$$

(see, for example, Prop. 1.5 of [2], where the definitions of the constants $s_2(L)$ and $A(L)$ are also given). It follows immediately that

$$\mathcal{E}_1^*(mz, L) - m\mathcal{E}_1^*(z, L) = \zeta(mz, L) - m\zeta(z, L).$$

But now we have the addition formula

$$\zeta(z_1 + z_2, L) = \zeta(z_1, L) + \zeta(z_2, L) + \frac{1}{2} \frac{\mathfrak{p}'(z_1, L) - \mathfrak{p}'(z_2, L)}{\mathfrak{p}(z_1, L) - \mathfrak{p}(z_2, L)}.$$

Taking the limit as z_1 tends to z_2 , we obtain the statement of the lemma for $m = 2$. For any $m \geq 2$, the above addition formula also shows that

$$\zeta((m+1)z, L) - (m+1)\zeta(z, L) = \zeta(mz, L) - m\zeta(z, L) + \frac{1}{2} \frac{\mathfrak{p}'(mz, L) - \mathfrak{p}'(z, L)}{\mathfrak{p}(mz, L) - \mathfrak{p}(z, L)},$$

whence the assertion of the lemma follows by induction on m . \square

The next lemma is attributed in [1] to unpublished notes of Swinnerton-Dyer.

Lemma 3.3. *Let w be any complex number such that w is not in L , but mw does belong to L for some integer $m \geq 2$. Then $\mathcal{E}_1^*(w, L) = -B_{m-1}(w, L)/m$.*

Proof. By the previous lemma, we have

$$B_{m-1}(w, L) = \mathcal{E}_1^*((m-1)w, L) - (m-1)\mathcal{E}_1^*(w, L).$$

But, as a function of z , $\mathcal{E}_1^*(z, L)$ is periodic with respect to L and odd, whence it follows that $\mathcal{E}_1^*((m-1)w, L) = -\mathcal{E}_1^*(w, L)$. This completes the proof. \square

Now we have the addition formula

$$\mathfrak{p}(z_1 + z_2, L) + \mathfrak{p}(z_1, L) + \mathfrak{p}(z_2, L) = \frac{1}{4} ((\mathfrak{p}'(z_1, L) - \mathfrak{p}'(z_2, L))/(\mathfrak{p}(z_1, L) - \mathfrak{p}(z_2, L)))^2,$$

whence we immediately obtain the following corollary.

Corollary 3.4. *Let w be any complex number such that w is not in L , but w does have finite order in \mathbb{C}/L . Let m be the exact order of w in \mathbb{C}/L . Assuming $m \geq 3$, we have*

$$m\mathcal{E}_1^*(w, L) = \sum_{k=1}^{k=m-2} \epsilon_k (\mathfrak{p}((k+1)w, L) + \mathfrak{p}(kw, L) + \mathfrak{p}(w, L))^{1/2},$$

where ϵ_k denotes the sign $+1$ or -1 .

We can now give the proof of Theorem 3.1. Recall that the period lattice of the Neron differential of our fixed global minimal Weierstrass equation (2) is $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$. Take $w = \psi(\mathfrak{b})\Omega_\infty/g_n$, where \mathfrak{b} is any fixed integral ideal of K prime to \mathfrak{g}_n . Thus $\mathcal{E}_1^*(w, \mathfrak{L})$ is any one of the conjugates of $\mathcal{E}_1^*(\Omega_\infty/g_n, \mathfrak{L})$ over K . Let m be the smallest positive rational integer lying in the ideal \mathfrak{g}_n , so that m is also the smallest positive rational integer with the property that mw lies in \mathfrak{L} . Moreover, since E has good reduction at the primes of K above 2, the ideal \mathfrak{f} is not divisible by any prime of K above 2. This means that the smallest positive rational integer in the ideal \mathfrak{g}_n must be odd. It follows that m is odd, and it must then be > 2 . Let P be the point on E defined by w . Then we have

$$(9) \quad \mathfrak{p}(rw, \mathfrak{L}) = x(rP) + (a_1^2 + 4a_2)/12, \quad (r = 1, \dots, m-1).$$

But, as E has good reduction at all primes of K above 2 and the point rP has odd order, it follows that $x(rP)$ is integral at each prime of \mathfrak{R}_n above 2. Thus we can immediately conclude from Corollary 3.4 and (9) that the following two assertions. Firstly, if $a_1/2$ lies in \mathcal{O}_K , then every conjugate of $\mathcal{E}_1^*(\Omega_\infty/g_n, \mathfrak{L})$ over K is integral at all places of \mathfrak{R}_n above 2. In general, if we drop the assumption that $a_1/2$ lies in \mathcal{O}_K , all we can say is that every conjugate of $2\mathcal{E}_1^*(\Omega_\infty/g_n, \mathfrak{L})$ over K is integral at every place of \mathfrak{R}_n above 2. Taken together, these two assertions clearly imply Theorem 3.1. \square

4 The induction argument

Let E be an elliptic curve defined over K , with complex multiplication by the ring of integers of K , and global minimal Weierstrass equation given by (2). We fix once and for all any place of the algebraic closure of \mathbb{Q} above 2, and write ord_2 for the order valuation at this place, normalized so that $\text{ord}_2(2) = 1$. Define α_E to be 0 or 1, according as 2 does or does not divide a_1 in \mathcal{O}_K , where we recall that a_1 is one of the coefficients in the equation (2). For any admissible sequence $\{\pi_1, \dots, \pi_n, \dots\}$ for E/K , we define $\mathfrak{M}_n = \pi_1 \dots \pi_n$, and

$$(10) \quad L^{(alg)}(\bar{\psi}_{\mathfrak{M}_n}, 1) = L(\bar{\psi}_{\mathfrak{M}_n}, 1) \sqrt{\mathfrak{M}_n}/\Omega_\infty,$$

which is an element of K . Moreover, we define

$$(11) \quad \phi_E = \alpha_E \text{ or } \max\{\alpha_E, -\text{ord}_2(L^{(alg)}(\bar{\psi}_E, 1))\},$$

according as $L(\bar{\psi}_E, 1) = 0$, or $L(\bar{\psi}_E, 1) \neq 0$. Our goal in this section is to prove the following theorem.

Theorem 4.1. *Assume that $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, and that E has good reduction at all places of K above 2. Then, for all admissible sequences $\{\pi_1, \dots, \pi_n, \dots\}$ for E/K , and all integers $n \geq 1$, we have*

$$(12) \quad \text{ord}_2(L^{(alg)}(\bar{\psi}_{\mathfrak{M}_n}, 1)) \geq n - \phi_E.$$

Proof. We shall prove the theorem by induction on n , and we begin with an obvious remark. Let r be any integer ≥ 0 , and recall that $\psi_{\mathfrak{M}_r}$ denotes the Grossencharacter of the twisted curve $E^{(\mathfrak{M}_r)}$. For each $n > r$, write $\mathfrak{p}_n = \pi_n \mathcal{O}_K$. Then \mathfrak{p}_n is prime to the conductor of $\psi_{\mathfrak{M}_r}$, and we have

$$(13) \quad \text{ord}_2(1 - \bar{\psi}_{\mathfrak{M}_r}(\mathfrak{p}_n)/N\mathfrak{p}_n) \geq 1.$$

Indeed, we have $\psi_{\mathfrak{M}_r}(\mathfrak{p}_n) = \zeta \pi_n$, where $\zeta = 1$ or -1 because $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. Thus $\zeta \equiv 1 \pmod{2}$, and (13) then follows easily because $\pi_n \equiv 1 \pmod{4}$ and $N\mathfrak{p}_n = \psi_{\mathfrak{M}_r}(\mathfrak{p}_n)\bar{\psi}_{\mathfrak{M}_r}(\mathfrak{p}_n)$. Note also that, on combining Theorems 3.1 and 2.4, we conclude that, for all integers $n \geq 1$, we have

$$(14) \quad \text{ord}_2\left(\sum_{M \in \mathcal{D}_n} L_{S_n}(\bar{\psi}_M, 1)/\Omega_\infty\right) \geq n - \alpha_E.$$

It is clear that, on combining (13) for $r = 0$ and (14) for $n = 1$, we immediately obtain (12) for $n = 1$. Suppose now that $n > 1$, and that (12) has been proven for all integers strictly less than n . Combining this inductive hypothesis with assertion (13), we conclude that for all proper divisors M of \mathfrak{M}_n , we have

$$\text{ord}_2(L_{S_n}(\bar{\psi}_M, 1)/\Omega_\infty) \geq n - \phi_E,$$

whence (14) again shows that (12) holds for the integer n . This completes the proof of the theorem. \square

We next investigate which rational primes p split in K , and have the additional property that they can be written as $p = \pi\pi^*$, with π in \mathcal{O}_K satisfying $\pi \equiv 1 \pmod{4}$ (and thus automatically also satisfying $\pi^* \equiv 1 \pmod{4}$). We call primes p with this property *special split primes* for K . Obviously, a necessary condition for p to be a special split prime for K is that $p \equiv 1 \pmod{4}$. We remark that it is clear from the Chebotarev density theorem that there are always infinitely many special split primes for K .

Lemma 4.2. *Assume that $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$. Let p be any rational prime which splits in K , and which satisfies $p \equiv 1 \pmod{4}$. If $K = \mathbb{Q}(\sqrt{-7})$, then p is always a special split prime for K . If $K = \mathbb{Q}(\sqrt{-q})$, where $q = 11, 19, 43, 67, 163$, then such a p is a special split prime for K if and only if we can write $p = \pi\pi^*$ in \mathcal{O}_K with $\pi + \pi^* \equiv 0 \pmod{2}$.*

Proof. Let $K = \mathbb{Q}(\sqrt{-q})$, and put $\tau = (1 + \sqrt{-q})/2$, so that $1, \tau$ form an integral basis of \mathcal{O}_K . Assume first that $K = \mathbb{Q}(\sqrt{-7})$. Then $p = a^2 + ab + 2b^2$, with a an odd integer, whose sign can be chosen so that $a \equiv 1 \pmod{4}$, and with b an even integer, which has necessarily

to be divisible by 4 since $p \equiv 1 \pmod{4}$. We then clearly have that $\pi = a + b\tau$ satisfies $\pi \equiv 1 \pmod{4}$. Finally, assume that $K = \mathbb{Q}(\sqrt{-q})$, where q is any of 11, 19, 43, 67, 163. Then $p = a^2 + ab + mb^2$, where a and b are integers, and $m = (q + 1)/4$ is now an odd integer. Since $p \equiv 1 \pmod{4}$, we see that $\pi = a + b\tau$ satisfies $\pi \equiv 1 \pmod{4}$ if and only if $a \equiv 1 \pmod{4}$ and b is even. But $\pi + \pi^* = 2a + b$, and so $\pi + \pi^*$ will be even if and only if b is even. By if b is even, then a is odd, and then we can always choose the sign of a so that $a \equiv 1 \pmod{4}$. This completes the proof. \square

Now assume that our elliptic curve E is in fact defined over \mathbb{Q} , and take (2) to be a global minimal Weierstrass equation for E over \mathbb{Q} . Then the conductor $N(E)$ of E is given by

$$N(E) = d_K N_{\mathfrak{f}},$$

where d_K denotes the absolute value of the discriminant of K . Moreover, the complex L -series $L(E, s)$ of E over \mathbb{Q} coincides with the Hecke L -series $L(\bar{\psi}_E, s)$. If R is a non-zero square free integer, $E^{(R)}$ will now denote the twist of E by the extension $\mathbb{Q}(\sqrt{R})/\mathbb{Q}$. Write

$$(15) \quad L^{(alg)}(E^{(R)}, 1) = L(E^{(R)}, 1) \sqrt{R} / \Omega_{\infty}.$$

Finally, α_E has the same definition as earlier, and ϕ_E is again defined by (11).

Lemma 4.3. *Assume that E is defined over \mathbb{Q} , and has complex multiplication by the ring of integers of any of the fields $K = \mathbb{Q}(\sqrt{-q})$, where $q = 7, 11, 19, 43, 67, 163$. Suppose further that E has good reduction at 2. Then the conductor $N(E)$ of E is a square.*

Proof. Let p be any prime dividing $N(E)$. Since E has potential good reduction at p , we must have that p^2 exactly divides $N(E)$ whenever $p > 3$. Also $p \neq 2$, because E has good reduction at 2. Thus we only have to check that an even power of 3 must divide $N(E)$. But, since $q > 3$, it is well known (see [3]) that E is the quadratic twist of an elliptic curve of conductor q^2 , whence it follows immediately that either 3 does not divide $N(E)$, or 3^2 exactly divides $N(E)$, according as 3 does not, or does, divide the discriminant of the twisting quadratic extension. This completes the proof. \square

We now introduce a definition which for the moment is motivated by what is needed to deduce the next theorem from our earlier induction argument (but see also the connexion with Tamagawa factors discussed in the next section). Write w_E for the sign in the functional equation of $L(E, s)$. We continue to assume that E is defined over \mathbb{Q} , and satisfies the hypotheses of Lemma 4.3. If D is any square free integer which is prime to $N(E)$, it is well known that the root number of the twist $E^{(D)}$ of E by the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is given by $\chi_D(-N(E))w_E$, where χ_D denotes the Dirichlet character of this quadratic extension. Thus, in view of Lemma 4.3, we are led to make the following definition.

Definition 4.4. Assume that E satisfies the hypotheses of Lemma . A square free positive integer M is said to be *admissible* for E if it satisfies (i) $(M, N(E)) = 1$, (ii) $M \equiv 1 \pmod{4}$ or $M \equiv 3 \pmod{4}$, according as $w_E = +1$ or $w_E = -1$, and (iii) every prime factor of M which splits in K is a special split prime for K .

Theorem 4.5. *Assume that E is defined over \mathbb{Q} , has complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-q})$, where $q = 7, 11, 19, 43, 67, 163$, and has good reduction at 2. Let M be a square free positive integer, which is admissible for E , and let $r(M)$ denote the number of primes of K dividing M . Put ϵ equal to $+1$ or -1 , according as $M \equiv 1$ or $3 \pmod{4}$. Then, for $w_E = \epsilon$, we have*

$$(16) \quad \text{ord}_2(L^{(\text{alg})}(E^{(\epsilon M)}, 1)) \geq r(M) - \phi_E.$$

Proof. Let M be any square free integer which is admissible for E , and let p be any prime dividing M . If p is inert in K , define π to be p or $-p$, according as p is congruent to 1 or $3 \pmod{4}$. If p splits in K , then Lemma 4.2 shows that we can then write $p = \pi\pi^*$, where π and π^* are elements of \mathcal{O}_K , which are both congruent to 1 $\pmod{4}$. Since every p with $p \equiv 3 \pmod{4}$, and p dividing M , is inert in K , it is now clear that we can write

$$\epsilon M = \pi_1 \dots \pi_{r(M)},$$

where the π_i are distinct prime elements of \mathcal{O}_K , which are all congruent to 1 $\pmod{4}$, and which are also prime to \mathfrak{f} and the discriminant of K . Hence the above theorem is an immediate consequence of Theorem 4.1. \square

The following is an immediate corollary of the above theorem. Of course, the hypothesis made in the corollary that $L(E, 1) \neq 0$ implies that the root number $w_E = 1$, and so the admissible M in this case are $\equiv 1 \pmod{4}$.

Corollary 4.6. *Assume that E is defined over \mathbb{Q} , has complex multiplication by the ring of integers of K , and has good reduction at 2. Suppose further that we have (i) $K \neq \mathbb{Q}(\sqrt{-3})$, (ii) $L(E, 1) \neq 0$, and (iii) $\text{ord}_2(L^{(\text{alg})}(E, 1)) < 0$. Let M be any square free positive integer which is admissible for E , and which is divisible only by rational primes which split in K . Then*

$$\text{ord}_2\left(\frac{L^{(\text{alg})}(E^{(M)}, 1)}{L^{(\text{alg})}(E, 1)}\right) \geq 2k(M),$$

where $k(M)$ denotes the number of rational prime divisors of M .

We now discuss some numerical examples of this theorem. For basic information about the curves discussed below, see, for example, [3]. As a first example, let E be the elliptic curve defined by

$$(17) \quad y^2 + xy = x^3 - x^2 - 2x - 1.$$

It has conductor 49, and complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-7})$. In fact, this curve is isomorphic to the modular curve $X_0(49)$. By the Chowla-Selberg formula, the period lattice \mathfrak{L} of the Neron differential on E is given by $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$, where

$$\Omega_\infty = \frac{\Gamma(\frac{1}{7})\Gamma(\frac{2}{7})\Gamma(\frac{4}{7})}{2\pi i \sqrt{-7}}.$$

Moreover, $\alpha_E = 1$ because $a_1 = 1$, and $L^{(alg)}(E, 1) = 1/2$, so that $\phi_E = 1$. Note that any positive square free integer M with $(M, 7) = 1$ and $M \equiv 1 \pmod{4}$, will be admissible for E , provided each of its prime factors which splits in K (thus a prime factor which is congruent to any of 1, 2, or 4 $\pmod{7}$) is congruent to 1 $\pmod{4}$. Theorem 4.5 therefore implies that, for such admissible integers M , we have

$$(18) \quad \text{ord}_2(L^{(alg)}(E^{(M)}, 1)) \geq r(M) - 1.$$

We see from Table I at the end of this paper that this estimate is in general best possible. As a second example, take for E the elliptic curve defined by

$$(19) \quad y^2 + y = x^3 - x^2 - 7x + 10.$$

It has conductor 121, and complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-11})$. Again by the Chowla-Selberg formula, the period lattice \mathfrak{L} of the Neron differential on E is given by $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$, where

$$\Omega_\infty = \frac{\Gamma(\frac{1}{11})\Gamma(\frac{3}{11})\Gamma(\frac{4}{11})\Gamma(\frac{5}{11})\Gamma(\frac{9}{11})}{2\pi i \sqrt{-11}}.$$

Moreover, $\alpha_E = 0$ because $a_1 = 0$, and $w_E = -1$, so that $\phi_E = 0$. The split primes for K are those which are congruent to 1, 3, 4, 5, 9 $\pmod{11}$. For example, all special split primes < 1000 for this curve are:-

$$53, 257, 269, 397, 401, 421, 617, 757, 773, 929.$$

Let now M be any square free positive integer which is admissible for E (in particular, since we are only interested in twists $E^{(-M)}$ having root number equal to +1, we assume that $M \equiv 3 \pmod{4}$ and $(M, 11) = 1$). Then Theorem 4.5 implies that

$$(20) \quad \text{ord}_2(L^{(alg)}(E^{(-M)}, 1)) \geq r(M).$$

However, in this example, Table II at the end of this paper suggests that this estimate is not, in general, best possible. It seems plausible to speculate from Table II that the lower bound of (20) could be improved to $r(M) + 1$.

5 Tamagawa Factors

Our goal in this last section is to relate the estimate given by Theorem 4.5 to the Tamagawa factors which arise in the Birch-Swinnerton-Dyer conjecture for the twists of our given elliptic curve with complex multiplication. Suppose first that E is any elliptic curve E defined over \mathbb{Q} , and any prime p of bad reduction for E , let $E(\mathbb{Q}_p)$ denote the group of points on E with coordinates in the field of p -adic numbers \mathbb{Q}_p , and $E_0(\mathbb{Q}_p)$ the subgroup of points with non-singular reduction modulo p . We define

$$\mathfrak{C}_p(E) = E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p),$$

and recall that the Tamagawa factor $c_p(E)$ is defined by

$$(21) \quad c_p(E) = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)].$$

If A is any abelian group, $A[m]$ will denote the kernel of multiplication by a positive integer m on A . The following lemma is very well known, but we give it for completeness.

Lemma 5.1. *Let E be any elliptic curve over \mathbb{Q} , and let p be a prime number where E has bad additive reduction. Then, for all positive integers m with $(m, p) = 1$, we have*

$$\mathfrak{C}_p(E)[m] = E(\mathbb{Q}_p)[m].$$

Proof. Let $E_1(\mathbb{Q}_p)$ denote the group of points on the formal group of E at p . Since E has additive reduction modulo p , the group of non-singular points on the reduction of E modulo p is isomorphic to the additive group of the field \mathbb{F}_p . As $E_1(\mathbb{Q}_p)$ is pro- p , and we have the exact sequence

$$0 \rightarrow E_1(\mathbb{Q}_p) \rightarrow E_0(\mathbb{Q}_p) \rightarrow \mathbb{F}_p \rightarrow 0,$$

it follows immediately that multiplication by m is an isomorphism on $E^0(\mathbb{Q}_p)$, whence the assertion of the lemma follows easily from a simple application of the snake lemma to the sequence

$$0 \rightarrow E_0(\mathbb{Q}_p) \rightarrow E(\mathbb{Q}_p) \rightarrow \mathfrak{C}_p(E) \rightarrow 0.$$

□

As earlier, let E now be our elliptic curve defined over \mathbb{Q} with complex multiplication by the ring of integers of the imaginary quadratic field K , and write $N(E)$ for the conductor of E . Once again, we will assume that E has good reduction at 2, and so we cannot have $K = \mathbb{Q}(\sqrt{-1})$, or $K = \mathbb{Q}(\sqrt{-2})$. Let M denote an odd positive square free integer with $(M, N(E)) = 1$. We put ϵ equal to $+1$ or -1 , according as M is congruent to 1 or 3 mod 4. Thus 2 is always unramified in the quadratic extension $\mathbb{Q}(\sqrt{\epsilon M})/\mathbb{Q}$.

Lemma 5.2. *Let p be any prime number dividing $N(E)$ or M . If p divides $N(E)$, then $\text{ord}_2(c_p(E^{(\epsilon M)})) = \text{ord}_2(c_p(E))$. If p divides M , then the value of $\text{ord}_2(c_p(E^{(\epsilon M)}))$ is independent of M .*

Proof. Let p be any prime factor of $N(E)$ or M , so that, in particular, p is odd. Since the j -invariant of E , and so also the j -invariant of $E^{(\epsilon M)}$, are integral, it follows from the table on p. 365 of [4] that the 2-primary subgroups of $\mathfrak{C}_p(E)$ and $\mathfrak{C}_p(E^{(\epsilon M)})$ are either 0, $\mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Now when p divides $N(E)$, both E and $E^{(\epsilon M)}$ have additive reduction at p , and so we conclude from Lemma 5.1 that, in this case,

$$\text{ord}_2(c_p(E)) = \text{ord}_2(\#(E(\mathbb{Q}_p)[2])), \text{ord}_2(c_p(E^{(\epsilon M)})) = \text{ord}_2(\#(E^{(\epsilon M)}(\mathbb{Q}_p)[2])),$$

Also when p divides M , we have, again from Lemma 5.1, that

$$(22) \quad \text{ord}_2(c_p(E^{(\epsilon M)})) = \text{ord}_2(\#(E^{(\epsilon M)}(\mathbb{Q}_p)[2])).$$

But the Galois group of $\mathbb{Q}(\sqrt{\epsilon M})/\mathbb{Q}$ clearly acts trivially on points of order 2 on $E^{(\epsilon M)}$, and so we always have

$$(23) \quad \#(E(\mathbb{Q}_p)[2]) = \#(E^{(\epsilon M)}(\mathbb{Q}_p)[2]).$$

The assertions of the lemma now follow immediately. \square

Theorem 5.3. *Assume that E is defined over \mathbb{Q} and has good reduction at 2, and that $K \neq \mathbb{Q}(\sqrt{-3})$. Let M be an odd positive square free integer with $(M, N(E)) = 1$, and having the property that every prime factor of M which is inert in K is congruent to 1 mod 4. Let p be any prime dividing M . Then (i) $\text{ord}_2(c_p(E^{(\epsilon M)})) = 1$ if p is inert in K , (ii) $\text{ord}_2(c_p(E^{(\epsilon M)})) = 0$ if p splits in K and the trace of the Frobenius endomorphism of the reduction of E modulo p is odd, and (iii) $\text{ord}_2(c_p(E^{(\epsilon M)})) = 2$ if p splits in K and the trace of the Frobenius endomorphism of the reduction of E modulo p is even.*

Before giving the proof of this theorem, we state an important corollary.

Corollary 5.4. *Assume that E is defined over \mathbb{Q} and has good reduction at 2, and that $K \neq \mathbb{Q}(\sqrt{-3})$. Let M be a positive integer which is admissible for E in the sense of Definition ??, and has the property that every prime factor of M is congruent to 1 mod 4. Write $r(M)$ for the number of primes divisors of M in K . Then*

$$(24) \quad \text{ord}_2\left(\prod_{p|M} c_p(E^{(\epsilon M)})\right) = r(M).$$

Proof. Let p be any prime factor of M . Since $(p, N(E)) = 1$, E has good reduction at p and p does not ramify in K . Recalling (22) and (23), we have to compute the order of $E(\mathbb{Q}_p)[2]$. Now, since p is odd, the Galois module $E[2]$ is unramified at p . Let \tilde{E} denote the reduction of E modulo p . Since the formal group of E at p is a \mathbb{Z}_p -module, it follows easily that reduction modulo p defines an isomorphism

$$E(\mathbb{Q}_p)[2] = \tilde{E}(\mathbb{F}_p)[2].$$

Now the order of $\tilde{E}(\mathbb{F}_p)$ is $1 + p$ or $1 - a_p + p$, according as p is inert or splits in K , where a_p is the trace of the Frobenius endomorphism of \tilde{E} . In particular, when p splits in K and a_p is odd, we see immediately that $E(\mathbb{Q}_p)[2] = 0$. Similarly, if p is inert in K , then, as $p \equiv 1 \pmod{4}$, we conclude that $E(\mathbb{Q}_p)[2]$ must have order 2. Suppose next that p splits in K and a_p is even. Let τ_p be any Frobenius automorphism at p . Since p splits in K , we can view τ_p as an element of the absolute Galois group of K , and we write ϕ_p for its image in the \mathcal{O}_K -automorphism group of the module $E[2]$, which is equal to $(\mathcal{O}_K/2\mathcal{O}_K)^*$. Then ϕ_p must have order dividing 2 because, since a_p is even, its characteristic polynomial is equal to $X^2 - 1$. But 2 is not ramified in K because E has good reduction at 2. Thus the group $(\mathcal{O}_K/2\mathcal{O}_K)^*$ has no element of order 2, whence we must have $\phi_p = 1$ and $E(\mathbb{Q}_p)[2] = E[2]$. The assertions of the theorem are now clear from (22) and (23). \square

Finally, we now compare some of our estimates with those predicted by the conjecture of Birch and Swinnerton-Dyer. The next proposition is an immediate consequence of Theorems 4.5 and 5.3.

Proposition 5.5. *Assume that E is defined over \mathbb{Q} and has good reduction at 2, and that $K \neq \mathbb{Q}(\sqrt{-3})$. Assume further that $L(E, 1) \neq 0$, and that $\text{ord}_2(L^{(\text{alg})}(E, 1)) < 0$. Then, for all positive integers M , which are admissible for E , and have the property that all of their prime factors are $\equiv 1 \pmod{4}$, we have*

$$(25) \quad \text{ord}_2\left(\frac{L^{(\text{alg})}(E^{(M)}, 1)}{L^{(\text{alg})}(E, 1)}\right) \geq \text{ord}_2\left(\prod_{p|M} c_p(E^{(M)})\right).$$

As we shall now explain, the lower bound given by (25) is exactly what the conjecture of Birch and Swinnerton-Dyer would predict for elliptic curves satisfying the hypotheses of this proposition. We first establish a preliminary result.

Proposition 5.6. *Let E be an elliptic curve defined over \mathbb{Q} , with complex multiplication by the ring of integers of K . Assume that E has good reduction at 2, and that $K \neq \mathbb{Q}(\sqrt{-3})$. Let M denote an odd positive square free integer with $(M, N(E)) = 1$, and put ϵ equal to $+1$ or -1 , according as M is congruent to 1 or $3 \pmod{4}$. Then the 2-primary subgroups of $E(\mathbb{Q})$ and $E^{(\epsilon M)}(\mathbb{Q})$ have the same order, and this order is equal to 2 or 1, according as the prime 2 splits or is inert in K .*

Proof. Let A denote the elliptic curve E or $E^{(\epsilon M)}(\mathbb{Q})$, so that A also has good reduction at 2. In order to show that the 2-primary subgroup of $A(\mathbb{Q})$ is annihilated by 2, it suffices to prove that the 2-primary subgroup of $A(K)$ is annihilated by 2. Now, as E has good reduction at 2, the prime 2 does not ramify in K , and thus it either splits or is inert in K . Let v denote any prime of K above 2. Since A has good reduction at v , the formal group of A at v is a Lubin-Tate formal group with parameter $\pi = \psi_A(v)$. Let n be any integer ≥ 1 . As the group $A[\pi^n]$ of π^n -division points on A lies on the formal group of A at v , it follows from Lubin-Tate theory the extension $K(A[\pi^n])/K$ has Galois group isomorphic to $(\mathcal{O}_K/\pi^n \mathcal{O}_K)^*$, which is non-trivial for all $n \geq 1$ if 2 is inert in K , and which is non-trivial for all $n \geq 2$ if 2 splits in K . In particular, the 2-primary subgroup of $A(K)$ must be trivial if 2 is inert in K , and it must be killed by 2 when 2 splits in K . But 2 splits in K happens precisely when $K = \mathbb{Q}(\sqrt{-7})$, and then A must be a quadratic twist of the curve given by (17). Now the curve (17) has a unique rational point of order 2 given by $(2, -1)$. It follows that $A(\mathbb{Q})$ must also have a unique point of order 2, because A is a quadratic twist of (17). This completes the proof. \square

Now assume that E satisfies the hypotheses of Proposition 5.5. Since $L(E, 1) \neq 0$, we know that both $E(\mathbb{Q})$ and the Tate-Shafarevich group of E/\mathbb{Q} are finite, and we write $w(E)$ and $t(E)$ for their respective orders. Then the conjecture of Birch and Swinnerton-Dyer predicts that

$$(26) \quad \text{ord}_2(L^{(\text{alg})}(E, 1)) = \text{ord}_2(c_\infty(E)) \prod_{p|N(E)} c_p(E) + \text{ord}_2(t(E)) - 2\text{ord}_2(w(E)).$$

where $c_\infty(E)$ denotes the number of connected components of $E(\mathbb{R})$. If we recall Proposition 5.6, and the fact that the Cassels-Tate theorem implies that $t(E)$ is the square of an integer, we see that the combination of our hypothesis that $\text{ord}_2(L^{(alg)}(E, 1)) < 0$ and the conjectural formula (26) imply that necessarily

$$(27) \quad \text{ord}_2(t(E)) = 0.$$

Suppose now that $L(E^{(M)}, 1) \neq 0$. Again, we then know that both $E^{(M)}(\mathbb{Q})$ and the Tate-Shafarevich group of $E^{(M)}/\mathbb{Q}$ are finite, and we write $w(E^{(M)})$ and $t(E^{(M)})$ for their respective orders. Then, in this case, the conjecture of Birch and Swinnerton-Dyer predicts that

$$(28) \quad \text{ord}_2(L^{(alg)}(E^{(M)}, 1)) = \text{ord}_2(c_\infty(E^{(M)})) \prod_{p|N(E)M} c_p(E^{(M)}) + \text{ord}_2(t(E^{(M)})) - 2\text{ord}_2(w(E^{(M)})).$$

where $c_\infty(E^{(M)})$ denotes the number of connected components of $E^{(M)}(\mathbb{R})$. Obviously, $c_\infty(E) = c_\infty(E^{(M)})$ since $\mathbb{Q}(\sqrt{M})$ is a real quadratic field. Moreover, Proposition 5.6 shows that $\text{ord}_2(w(E)) = \text{ord}_2(w(E^{(M)}))$, and Lemma 5.2 tells us that, for primes p dividing $N(E)$, we have $\text{ord}_2(c_p(E)) = \text{ord}_2(c_p(E^{(M)}))$. Hence, recalling (27), we conclude that the conjecture of Birch and Swinnerton-Dyer predicts that

$$(29) \quad \text{ord}_2\left(\frac{L^{(alg)}(E^{(M)}, 1)}{L^{(alg)}(E, 1)}\right) = \text{ord}_2\left(\prod_{p|M} c_p(E^{(M)})\right) + \text{ord}_2(t(E^{(M)})).$$

This shows that, under the above hypotheses, the lower bound given by (25) is precisely what the conjecture of the Birch and Swinnerton-Dyer would predict if we ignore the unknown term $\text{ord}_2(t(E^{(M)}))$ giving the order of the 2-primary subgroup of the Tate-Shafarevich group of the curve $E^{(M)}$.

6 Tables

In this section, we include some short tables of numerical examples of our results for two elliptic curves E defined over \mathbb{Q} . We use the same notation as earlier. For the curve of conductor 49 in Table I, the root number of the curve is $+1$, and for the curve of conductor 121 in Table II the root number is -1 . As always, M will denote a square free positive integer which is admissible for the elliptic curve E , and $r(M)$ will denote the number of prime divisors of M in the field of complex multiplication K .

Table I: Case $X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1$. The Tamagawa factor of twists $E^{(M)}$ at 7 is always 2. $L^{(alg)}(E, 1) = 1/2$.					
M	$L(E^{(M)}, 1)$	$L^{(alg)}(E^{(M)}, 1)$	$ord_2 L^{(alg)}(E^{(M)}, 1)$	$r(M)$	Tamagawa Factors
29	0.7180139420	2	1	2	$c_{29} = 4$,
37	0.6356689731	2	1	2	$c_{37} = 4$,
109	0.3703553538	2	1	2	$c_{109} = 4$,
113	1.454965333	8	3	2	$c_{113} = 4$,
137	0.3303479321	2	1	2	$c_{137} = 4$,
145	0.6422111932	4	2	3	$c_5 = 2$, $c_{29} = 4$,
185	2.274238456	16	4	3	$c_5 = 2$, $c_{37} = 4$,
233	2.279798298	18	1	2	$c_{233} = 4$,
265	4.275446184	36	2	3	$c_5 = 2$, $c_{53} = 4$,
277	0.9292915388	8	3	2	$c_{277} = 4$,
281	0.2306634143	2	1	2	$c_{281} = 4$,
285	1.832312031	16	4	3	$c_3 = 2$, $c_5 = 2$, $c_{19} = 2$,
317	0.8686848279	8	3	2	$c_{317} = 4$,
337	0.2106283985	2	1	2	$c_{337} = 4$,
377	0.3982824745	4	2	3	$c_{13} = 2$, $c_{29} = 4$,
389	1.764410302	18	1	2	$c_{389} = 4$,
401	1.737809629	18	1	2	$c_{401} = 4$,
421	0.7537907774	8	3	2	$c_{421} = 4$,
449	2.919635854	32	5	2	$c_{449} = 4$,
457	0.7234920569	8	3	2	$c_{457} = 4$,
481	1.410422816	16	4	3	$c_{13} = 2$, $c_{37} = 4$,
545	0.3312558988	4	2	3	$c_5 = 2$, $c_{109} = 4$,
557	0.6553363680	8	3	2	$c_{557} = 4$,
565	0.3253401390	4	2	3	$c_5 = 2$, $c_{113} = 4$,
569	0.1620972858	2	1	2	$c_{569} = 4$,
613	0.1561714487	2	1	2	$c_{613} = 4$,
617	0.1556643972	2	1	2	$c_{617} = 4$,
629	1.233378974	16	4	3	$c_{17} = 2$, $c_{37} = 4$,
641	0.1527224426	2	1	2	$c_{641} = 4$,
653	0.1513126668	2	1	2	$c_{653} = 4$,
673	1.341426413	18	1	2	$c_{673} = 4$,
701	0.1460403507	2	1	2	$c_{701} = 4$,
705	1.165003700	16	4	3	$c_3 = 2$, $c_5 = 2$, $c_{47} = 2$,
709	0.1452140903	2	1	2	$c_{709} = 4$,
757	0.1405348183	2	1	2	$c_{757} = 4$,

Table I: Case $X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1$.					
M	$L(E^{(M)}, 1)$	$L^{(alg)}(E^{(M)}, 1)$	$ord_2 L^{(alg)}(E^{(M)}, 1)$	$r(M)$	Tamagawa Factors
809	0.5437729586	8	3	2	$c_{809} = 4$,
821	0.5397843500	8	3	2	$c_{821} = 4$,
877	1.175099358	18	1	2	$c_{877} = 4$,
901	1.030527220	16	4	3	$c_{17} = 2$, $c_{53} = 4$,
953	0.5010088727	8	3	2	$c_{953} = 4$,
965	0.2489420234	4	2	3	$c_5 = 2$, $c_{193} = 4$,
969	0.9937107192	16	4	3	$c_3 = 2$, $c_{17} = 2$, $c_{19} = 2$,
977	1.113338183	18	1	2	$c_{977} = 4$,
985	2.217615590	36	2	3	$c_5 = 2$, $c_{197} = 4$,

Table II: Case $E : y^2 + y = x^3 - x^2 - 7x + 10$ of conductor 121. The Tamagawa factor of twists $E^{(-M)}$ at 11 is always 2.					
M	$ L(E^{(-M)}, 1) $	$ L^{(alg)}(E^{(-M)}, 1) $	$ord_2 L^{(alg)}(E^{(-M)}, 1) $	$r(M)$	Tamagawa factors
7	1.094573405	4	2	1	$c_7 = 2$,
43	0.4416311353	4	2	1	$c_{43} = 2$,
79	0.3258219706	4	2	1	$c_{79} = 2$,
83	0.3178738964	4	2	1	$c_{83} = 2$,
107	0.2799638923	4	2	1	$c_{107} = 2$,
119	0.5309460896	8	3	2	$c_7 = 2$, $c_{17} = 2$,
127	1.027902784	16	4	1	$c_{127} = 2$,
131	0.2530219881	4	2	1	$c_{131} = 2$,
139	0.2456328864	4	2	1	$c_{139} = 2$,
151	0.2356706165	4	2	1	$c_{151} = 2$,
203	0.4065143570	8	3	2	$c_7 = 2$, $c_{29} = 2$,
211	0.7974669169	16	4	1	$c_{211} = 2$,
227	0.1922122148	4	2	1	$c_{227} = 2$,
239	0.1873246635	4	2	1	$c_{239} = 2$,
247	0.3685321923	8	3	2	$c_{13} = 2$, $c_{19} = 2$,
263	0.1785730998	4	2	1	$c_{263} = 2$,
271	0.7036703591	16	4	1	$c_{271} = 2$,
287	0.3418872925	8	3	2	$c_7 = 2$, $c_{41} = 2$,
307	2.644506912	64	6	1	$c_{307} = 2$,
323	0.3222720533	8	3	2	$c_{17} = 2$, $c_{19} = 2$,
347	0.6218550501	16	4	1	$c_{347} = 2$,
371	0.6014048805	16	4	3	$c_7 = 2$, $c_{53} = 4$,
427	0.2802915271	8	3	2	$c_7 = 2$, $c_{61} = 2$,
431	0.1394939193	4	2	1	$c_{431} = 2$,
439	0.5528682408	16	4	1	$c_{439} = 2$,

Table II: Case $X_0(121) : y^2 + y = x^3 - x^2 - 7x + 10$.					
M	$ L(E^{(-M)}, 1) $	$ L^{(alg)}(E^{(-M)}, 1) $	$ord_2 L^{(alg)}(E^{(-M)}, 1) $	$r(M)$	Tamagawa factors
491	0.5227730093	16	4	1	$c_{491} = 2,$
503	0.1291248765	4	2	1	$c_{503} = 2,$
511	0.2562202539	8	3	2	$c_7 = 2, c_{73} = 2,$
547	1.981163103	64	6	1	$c_{547} = 2,$
551	0.2467448562	8	3	2	$c_{19} = 2, c_{29} = 2,$
559	0.2449728774	8	3	2	$c_{13} = 2, c_{43} = 2,$
563	0.4882021701	16	4	1	$c_{563} = 2,$
607	1.057893809	36	2	1	$c_{607} = 2,$
659	0.1128109364	4	2	1	$c_{659} = 2,$
707	0.8713129959	32	5	2	$c_7 = 2, c_{101} = 2,$
731	0.2142225669	8	3	2	$c_{17} = 2, c_{43} = 2,$
739	0.1065299425	4	2	1	$c_{739} = 2,$
743	0.4249711969	16	4	1	$c_{743} = 2,$
763	0.8387289424	32	5	2	$c_7 = 2, c_{109} = 2,$
787	1.651682351	64	6	1	$c_{787} = 2,$
811	0.9152210367	36	2	1	$c_{811} = 2,$
887	0.09723712323	4	2	1	$c_{887} = 2,$
919	0.09552920333	4	2	1	$c_{919} = 2,$

References

- [1] R. DAMERELL, *L-functions of elliptic curves with complex multiplication II*, Acta Arithmetica **19** (1971), 311-317.
- [2] C. GOLDSTEIN, N. SCHAPPACHER, *Series d'Eisenstein et fonctions L de courbes elliptiques a multiplication complexe*, Crelle **327** (1981), 184-218.
- [3] B. GROSS, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Math. **776** (1980), Springer.
- [4] J. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts Math. 151 (1994), Springer.
- [5] K. RUBIN, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25-68.
- [6] Y. TIAN, *Congruent numbers with many prime factors*, Proc. Natl. Acad. Sci. USA **109**(2012), 21256-21258.
- [7] Y. TIAN, *Congruent numbers and Heegner points*, to appear.
- [8] Y. TIAN, X. YUAN, S. ZHANG, *Heegner number problems and L-functions*, to appear.

- [9] C. ZHAO, *A criterion for elliptic curves with lowest 2-power order in $L(1)$* , Proc. Cambridge Phil. Soc. **121** (1997), 385-400.
- [10] C. ZHAO, *A criterion for elliptic curves with second lowest 2-power order in $L(1)$* , Proc. Cambridge Phil. Soc. **131** (2001), 385-404.
- [11] C. ZHAO, *A criterion for elliptic curves with second lowest 2-power order in $L(1)$ (II)*, Proc. Cambridge Phil. Soc. **134** (2003), 407-420.
- [12] C. ZHAO, *A criterion for elliptic curves with second lowest 2-power order in $L(1)$ (III)*, Acta Mathematica Sinica, **21** (2005), 961-976.

J.C: Emmanuel College, Cambridge, England, and Department of Mathematics, POSTECH, Pohang, South Korea, email: `jhc13@dpms.cam.ac.uk`

M.K: Merton College, Oxford, England, email: `Minhyong.Kim@maths.ox.ac.uk`

Z.L: School of Mathematical Sciences, Capital Normal University, and Beijing International Center for Mathematical Research, Peking University, Beijing, People's Republic of China, email: `liangzhib@gmail.com`

C.Z.: Department of Mathematics, Peking University, Beijing, People's Republic of China, email: `zhao@math.pku.edu.cn`